

On the covering radius of first order generalized Reed-Muller codes

Elodie Leducq*

1 Introduction

The determination of the covering radius of the first order Reed-Muller code is a difficult problem in coding theory. In this paper, we generalize to any q some results proved in [1, 4, 6, 7] for $q = 2$.

Let $q = p^t$, p a prime number.

Let $B_m^q = \mathbb{F}_q[X_1, \dots, X_m]/(X_1^q - X_1, \dots, X_m^q - X_m)$; B_m^q actually consists of all the functions from \mathbb{F}_q^m to \mathbb{F}_q . We identify B_m^q with $\mathbb{F}_q^{q^m}$ through the application

$$\begin{aligned} B_m^q &\rightarrow \mathbb{F}_q^{q^m} \\ P &\mapsto (P(x))_{x \in \mathbb{F}_q^m} \end{aligned}$$

For all $b \in \mathbb{F}_q^m$, we denote by 1_b the function in B_m^q such that $1_b(b) = 1$ and for all $x \neq b$, $1_b(x) = 0$.

The weight $|P|$ of $P \in B_m^q$ is $\text{Card}(\{x, P(x) \neq 0\})$. The Hamming distance in B_m^q is denoted by $d(., .)$.

For $0 \leq r \leq m(q-1)$, the r th order generalized Reed-Muller code of length q^m is

$$R_q(r, m) = \{P \in B_m^q, \deg(P) \leq r\}$$

where $\deg(P)$ is the degree of the representant of P with degree at most $q-1$ in each variable (see [8]). For all $0 \leq r \leq m(q-1)$, the affine group $\text{GA}_m(\mathbb{F}_q)$ acts on $R_q(r, m)$ by its natural action and we have

Proposition 1 (see [8])

For all q , for all $m \geq 0$ and $1 \leq r \leq m(q-1) - 2$,

$$\text{Aut}(R_q(r, m)) = \text{GA}_m(\mathbb{F}_q).$$

The covering radius of a code C of length n is

$$\rho(C) = \max_{x \in \mathbb{F}_q^n} \min_{c \in C} |x - c|$$

We denote by $\rho(r, m)$ the covering radius of $R_q(r, m)$.

For $q = 2$, $\rho(1, m)$ are unknown for m odd, $m \geq 9$. We know that $\rho(1, 5) = 12$ and $\rho(1, 7) = 56$ (see [1, 6]).

Since $R_q(1, m) \subset R_q(2, m) \subset \dots \subset R_q(m(q-1), m) = \mathbb{F}_q^{q^m}$, we can try to study $\rho(1, m)$ through the covering radius of $R_q(1, m)$ in $R_q(r, m)$, $2 \leq r \leq m(q-1)$. We define

$$\rho_r(1, m) = \max_{x \in R_q(r, m)} \min_{c \in R_q(1, m)} |x - c|$$

For $q = 2$, it is known that $\rho_2(1, m) = 2^{m-1} - 2^{\lceil \frac{m}{2} \rceil - 1}$ (see [7]) which gives $\rho(1, m) \geq 2^{m-1} - 2^{\lceil \frac{m}{2} \rceil - 1}$ and, since $\rho(1, m) \leq 2^{m-1} - 2^{\frac{m}{2} - 1}$ (see [4]), we get, for m even $\rho(1, m) = 2^{m-1} - 2^{\frac{m}{2} - 1}$.

In part 2, we give a general upper bound for covering radius of codes over \mathbb{F}_q .

Then we calculate $\rho_2(1, m)$:

*IMJ, preparing a PhD thesis under direction of Jean-françois Mestre

Theorem 2 For all $q, m \geq 0$,

$$\rho_2(1, m) = (q-1)q^{m-1} - q^{\lceil \frac{m}{2} \rceil - 1}.$$

We use previous results to give an upper bound and a lower bound for $\rho(1, m)$, which give $\rho(1, m)$ when m is even :

Theorem 3 For all $q, m \geq 0$,

$$(q-1)q^{m-1} - q^{\lceil \frac{m}{2} \rceil - 1} \leq \rho(1, m) \leq (q-1)q^{m-1} - q^{\frac{m}{2} - 1}.$$

Furthermore, we get functions, f , such that $d(f, R(1, m)) = \rho(1, m)$ when m is even. Finally, we study more precisely the case where $q = 3$.

2 A general upper bound

We need to extend the definition of self-complementary code and the definition of strength of a code for a binary code (see [4]) to a code over \mathbb{F}_q .

Definition 4 A code C over \mathbb{F}_q is self-complementary if

$$\forall c \in C, \forall \omega \in \mathbb{F}_q, \tilde{c}^\omega = (\omega, \dots, \omega) + c \in C.$$

Definition 5 A code C over \mathbb{F}_q has strength s if each s -subset of coordinates of the code contains all elements of \mathbb{F}_q^s a constant number of times.

Now, we generalize the upper bound of covering radius of a binary code given in [4] to codes over \mathbb{F}_q .

Lemma 6 Let C be a code over \mathbb{F}_q of length n , and let $v \in \mathbb{F}_q^m$. If C has strength 2, then

$$\sum_{u \in v+C} |u|^2 = n \left(\frac{q-1}{q} \right) \left((n-1) \left(\frac{q-1}{q} \right) + 1 \right) \text{Card}(C)$$

Proof : $v + C$ has strength 2 if and only if C has strength 2.

Furthermore, $\text{Card}(v + C) = \text{Card}(C)$, so it is enough to prove the lemma for $v = 0$.

$$\begin{aligned} \sum_{u \in C} |u|^2 &= \sum_{u \in C} \sum_{i, u_i \neq 0} \sum_{j, u_j \neq 0} 1 = \sum_{u \in C} \sum_{i, u_i \neq 0} \sum_{j \neq i, u_j \neq 0} 1 + \sum_{u \in C} \sum_{i, u_i \neq 0} 1 \\ &= \sum_{i=1}^n \sum_{j \neq i} \sum_{u \in C, u_i u_j \neq 0} 1 + \sum_{i=1}^n \sum_{u \in C, u_i \neq 0} 1 \end{aligned}$$

Since C has strength 2, $\sum_{u \in C, u_i u_j \neq 0} 1 = \left(\frac{q-1}{q} \right)^2 \text{Card}(C)$

and $\sum_{u \in C, u_i \neq 0} 1 = \left(\frac{q-1}{q} \right) \text{Card}(C)$.

Hence $\sum_{u \in C} |u|^2 = n(n-1) \left(\frac{q-1}{q} \right)^2 \text{Card}(C) + n \left(\frac{q-1}{q} \right) \text{Card}(C)$.

□

Theorem 7 If C is a self-complementary code over \mathbb{F}_q of length n and strength 2, then

$$\rho(C) \leq \frac{(q-1)}{q}n - \frac{\sqrt{n}}{q}.$$

Proof : Let $v \in \mathbb{F}_q^n$ such that its distance to any codeword is at least r , i.e. $\forall u \in v + C, |u| \geq r$. Since C is self-complementary, if $u \in v + C$ then $\bar{u}^\omega \in v + C$ and $|\bar{u}^\omega| \geq r$.

We have :

$$\sum_{\omega \in \mathbb{F}_q} |\bar{u}^\omega| = \sum_{\omega \in \mathbb{F}_q} (|u| - x_{-\omega} + x_0) = q(|u| + x_0) - \sum_{\omega \in \mathbb{F}_q} x_{-\omega} = (q-1)n$$

where $x_\omega = \text{Card}(\{i, u_i = \omega\})$.

Assume $r > \frac{q-1}{q}n$, so

$$\frac{q-1}{q}n < r \leq |u| = n(q-1) - \sum_{\omega \in \mathbb{F}_q^*} |\bar{u}^\omega| \leq n(q-1) - (q-1)r < \frac{q-1}{q}n.$$

We get a contradiction. So we write $r = \frac{q-1}{q}n - \rho$ with $\rho \geq 0$ and we have :

$$\begin{aligned} \sum_{\omega \in \mathbb{F}_q} |\bar{u}^\omega|^2 &= \sum_{\omega \in \mathbb{F}_q^*} |\bar{u}^\omega|^2 + |u|^2 \\ &= \sum_{\omega \in \mathbb{F}_q^*} |\bar{u}^\omega|^2 + \left((q-1)n - \sum_{\omega \in \mathbb{F}_q^*} |\bar{u}^\omega| \right)^2 \\ &\leq (q-1)r^2 + (q-1)^2(n-r)^2 \\ &= (q-1) \left(\frac{q-1}{q}n - \rho \right)^2 + (q-1)^2 \left(\frac{n}{q} + \rho \right)^2 \\ &= q \left(n^2 \frac{(q-1)^2}{q^2} + (q-1)\rho^2 \right) \end{aligned}$$

we get

$$\sum_{u \in v+C} |u|^2 \leq \left(n^2 \frac{(q-1)^2}{q^2} + (q-1)\rho^2 \right) \text{Card}(C).$$

And, from lemma 6,

$$n^2 \frac{(q-1)^2}{q^2} + n \frac{(q-1)}{q^2} \leq \left(n^2 \frac{(q-1)^2}{q^2} + (q-1)\rho^2 \right).$$

Hence $\frac{n}{q^2} \leq \rho^2$, and so, since $\rho \geq 0$, $r \leq \frac{(q-1)}{q}n - \frac{\sqrt{n}}{q}$.

Theorem 7 follows from the definition of covering radius. □

3 Counting zeros of quadratic forms

Definition 8 We say that an application from \mathbb{F}_q^m to \mathbb{F}_q is a quadratic form if

1. $Q(ax) = a^2 Q(x)$ for $a \in \mathbb{F}_q$ and $x \in \mathbb{F}_q^m$.
2. $\phi : \mathbb{F}_q^m \times \mathbb{F}_q^m \rightarrow \mathbb{F}_q$ such that $\phi(x, y) = Q(x+y) - Q(x) - Q(y)$ is a bilinear form.

ϕ is called the bilinear form associated to Q .

Definition 9 We called rank of a bilinear form ϕ , the rank of the following application

$$\psi_\phi : \begin{array}{ccc} \mathbb{F}_q^n & \rightarrow & \mathbb{F}_q^{m*} \\ x & \mapsto & (y \mapsto \phi(x, y)) \end{array}$$

Let Q be a quadratic form over \mathbb{F}_q^n and ϕ the associated bilinear form.

Let $V = \{x \in \text{Ker}(\psi_\phi), Q(x) = 0\}$ and let $v = \dim(V) \leq n - \text{Rg}(\phi)$, then we define the rank of Q by $\text{Rg}(Q) = n - v$.

We say that Q is non degenerate, if $v = 0$.

Remark : If q is odd, then $v = n - \text{Rg}(\phi)$ and $\text{Rg}(\phi) = \text{Rg}(Q)$.

We need the following theorem about reduction of quadratic forms :

Theorem 10 *Let Q be a quadratic form of rank R on \mathbb{F}_q^n , then there exists a basis $(e_i)_{1 \leq i \leq n}$ of \mathbb{F}_q^n such that :*

- If $R = 2s + 1$, then $Q(\sum_{i=1}^n x_i e_i) = \sum_{i=1}^s x_{2i-1} x_{2i} + a x_{2s+1}^2$ (1)
 - If $R = 2s$, then $Q(\sum_{i=1}^n x_i e_i) = \sum_{i=1}^s x_{2i-1} x_{2i}$ (2)
- or $Q(\sum_{i=1}^n x_i e_i) = \sum_{i=1}^s x_{2i-1} x_{2i} + a x_{2s-1}^2 + b x_{2s}^2 + c x_{2s-1} x_{2s}$ where $ax^2 + cx + b$ is irreducible over \mathbb{F}_q (3)

Proof : Let ϕ be the bilinear form associated to Q .

Let $N = \{x, \forall y \in \mathbb{F}_q^n, \phi(x, y) = 0\}$ and S be a subspace supplementary to N in \mathbb{F}_q^n .

Let $V_0 = \{x \in N, Q(x) = 0\}$ and let V_1 be a subspace supplementary to V_0 in N .

So Q restricted to $V_1 \oplus S$ is non degenerate.

If q is even, see [3] p.33-34 and [2] p.197-199.

If q is odd, see [5] p.117-118 and p.121-123.

□

Now, we can count zeros of quadratic forms (see [5]) :

Theorem 11 *Let Q be a quadratic form over \mathbb{F}_q^n of rank R , then the number of zeros of Q is*

$$N(Q) = q^{n-1} + (\omega - 1)(q - 1)q^{n-\frac{R}{2}-1}$$

$$\text{where } \omega = \begin{cases} 1 & \text{if } R \text{ is odd} \\ 2 & \text{if } R \text{ is even and } Q \text{ is of type (2) (see theorem 10)} \\ 0 & \text{if } R \text{ is even and } Q \text{ is of type (3)} \end{cases}$$

Proof : If $R = 0$, there are q^n zeros.

If $R = 1$, we can write $Q = ax_1^2$, and so Q has q^{n-1} zeros.

If $R = 2$, we can write $Q = ax_1^2 + bx_2^2 + cx_1 x_2$.

If $ax^2 + cx + b$ is irreducible, we are in case (3) and Q has $q^{n-2} = q^{n-1} - (q-1)q^{n-\frac{2}{2}-1}$ zeros. Otherwise, Q factors, so we are in case (2), and Q has $(2q-1)q^{n-2} = q^{n-1} + (q-1)q^{n-\frac{2}{2}-1}$ zeros.

If $R \geq 3$, by theorem 10, we can write $Q = x_1 x_2 + Q^{(1)}(x_3, \dots, x_n)$ where $Q^{(1)}$ is a quadratic form of rank $R - 2$.

If $Q^{(1)}(a_3, \dots, a_n) = 0$, then there are $(2q-1)$ couples (x_1, x_2) such that $Q(x_1, x_2, a_3, \dots, a_n) = 0$.

Otherwise, there are $(q-1)$ couples (x_1, x_2) such that $Q(x_1, x_2, a_3, \dots, a_n) = 0$.

Hence

$$N(Q) = (2q-1)N(Q^{(1)}) + (q-1)(q^{n-2} - N(Q^{(1)})) = qN(Q^{(1)}) + (q-1)q^{n-2}.$$

Continuing this process, we get, for r such that $R - 2r \geq 1$

$$\begin{aligned} N(Q) &= q^r N(Q^{(r)}) + (q-1)(q^{n-2} + q^{n-3} + \dots + q^{n-(r+1)}) \\ &= q^r N(Q^{(r)}) + q^{n-1} - q^{n-(r+1)} \end{aligned}$$

where $Q^{(r)}$ is a quadratic form in x_{2r+1}, \dots, x_n with rank $R - 2r$.

If R is odd, we put $R = 2s + 1$ and $r = s$, then we get $N(Q) = q^s q^{n-2s-1} + q^{n-1} - q^{n-s-1} = q^{n-1}$ since $Q^{(s)}$ is a quadratic form in $n - 2s$ variables, with rank 1. That gives the theorem in the case where R is odd.

If R is even, we put $R = 2s$ and $r = s - 1$, then $Q^{(s-1)}$ is a quadratic form in $n - 2s + 2$ variables of rank 2. If Q is of type (3), $Q^{(s-1)}$ does not factor and has q^{n-2s} zeros. So

$N(Q) = q^{s-1} q^{n-2s} + q^{n-1} - q^{n-s} = q^{n-1} - (q - 1)q^{n-s-1}$. If Q is of type (2), $Q^{(s-1)}$ factors and has $(2q - 1)q^{n-2s}$ zeros. So $N(Q) = q^{s-1}(2q - 1)q^{n-2s} + q^{n-1} - q^{n-s} = q^{n-1} + (q - 1)q^{n-s-1}$.

□

Now we are able to prove theorem 2.

4 Proof of theorem 2

Let $q_0 = \sum_{1 \leq i \leq j \leq m} a_{i,j} x_i x_j$

In order to get the weight of $q_0 + \alpha_1 x_1 + \dots + \alpha_m x_m + \beta$, we homogenize :

let $Q = q_0 + \alpha_1 x_1 z + \dots + \alpha_m x_m z + \beta z^2$.

We denote by N_q^∞ , the number of zeros of q_0 in \mathbb{F}_q^m , which is the number of infinite points of the quadric defined by $Q = 0$ and by N_q , the number of zeros of Q in \mathbb{F}_q^{m+1} .

Then the number of zeros of $q_0 + \alpha_1 x_1 + \dots + \alpha_m x_m + \beta$, N , is the number of point of the quadric which are not infinite points, so we get

$$N = \frac{N_q - N_q^\infty}{q - 1}.$$

By theorem 11 we have :

$$N_q^\infty = q^{m-1} + q^{m-\frac{r}{2}-1}(q-1)(\omega_{q_0} - 1)$$

where $r = \text{rg}(q_0)$ and

$$\omega_{q_0} = \begin{cases} 1 & \text{if } r \text{ is odd} \\ 2 & \text{if } r \text{ is even and } q_0 \text{ is of type (2)} \\ 0 & \text{if } r \text{ is even and } q_0 \text{ is of type (3)} \end{cases}$$

and

$$N_q = q^m + q^{m-\frac{R}{2}}(q-1)(\omega_Q - 1)$$

where $R = \text{rg}(Q)$ and

$$\omega_Q = \begin{cases} 1 & \text{if } R \text{ is odd} \\ 2 & \text{if } R \text{ is even and } Q \text{ is of type (2)} \\ 0 & \text{if } R \text{ is even and } Q \text{ is of type (3)} \end{cases}$$

So, the number of zeros of $q_0 + \alpha_1 x_1 + \dots + \alpha_m x_m + \beta$ is

$$N = q^{m-1} - (\omega_{q_0} - 1)q^{m-\frac{r}{2}-1} + (\omega_Q - 1)q^{m-\frac{R}{2}}.$$

Hence

$$|q_0 + \alpha_1 x_1 + \dots + \alpha_m x_m + \beta| = (q-1)q^{m-1} + (\omega_{q_0} - 1)q^{m-\frac{r}{2}-1} - (\omega_Q - 1)q^{m-\frac{R}{2}}.$$

Then we want to calculate $d(q_0, R_q(1, m))$:

- If r is odd, $\omega_{q_0} = 1$, $|q_0 + \alpha_1 x_1 + \dots + \alpha_m x_m + \beta| = (q-1)q^{m-1} - (\omega_Q - 1)q^{m-\frac{R}{2}}$ and q_0 can be reduced to $x_1 x_2 + \dots + x_{r-2} x_{r-1} + a x_r^2$ by a linear transformation, which does not change the

weight, so we can assume that

$$\begin{aligned}
Q &= x_1x_2 + \dots + x_{r-2}x_{r-1} + ax_r^2 + \alpha_1x_1z + \dots + \alpha_mx_mz + \beta z^2 \\
&= (x_1 + \alpha_2z)(x_2 + \alpha_1z) + \dots + (x_{r-2} + \alpha_{r-1}z)(x_{r-1} + \alpha_{r-2}z) + ax_r^2 \\
&\quad + z(\alpha_rx_r + \dots + \alpha_mx_m) + \underbrace{(\beta - \alpha_1\alpha_2 - \dots - \alpha_{r-2}\alpha_{r-1})}_{\theta} z^2 \\
&= (x_1 + \alpha_2z)(x_2 + \alpha_1z) + \dots + (x_{r-2} + \alpha_{r-1}z)(x_{r-1} + \alpha_{r-2}z) + ax_r^2 \\
&\quad + z(\alpha_rx_r + \dots + \alpha_mx_m + \theta z)
\end{aligned}$$

If there exists $i > r$ such that $\alpha_i \neq 0$, then $R = r + 2$ and $\omega_Q = 1$.

If for all $i > r$, $\alpha_i = 0$:

If $\theta \neq 0$, then $R = r + 1$ and $\omega_Q = \begin{cases} 0 & \text{if } ax^2 + \alpha_rx + \theta \text{ is irreducible} \\ 2 & \text{otherwise} \end{cases}$

If $\theta = 0$, then, if $\alpha_r = 0$, $R = r$ and $\omega_Q = 1$. Otherwise, $R = r + 1$ and $\omega_Q = 2$.

Hence $d(q_0, R_q(1, m)) = (q - 1)q^{m-1} - q^{m-\frac{r+1}{2}}$.

- If r is even and $\omega_{q_0} = 2$, $|q_0 + \alpha_1x_1 + \dots + \alpha_mx_m + \beta| = (q - 1)q^{m-1} + q^{m-\frac{r}{2}-1} - (\omega_Q - 1)q^{m-\frac{r}{2}}$ and q_0 can be reduced to $x_1x_2 + \dots + x_{r-1}x_r$ by a linear transformation.

$$\begin{aligned}
Q &= x_1x_2 + \dots + x_{r-1}x_r + \alpha_1x_1z + \dots + \alpha_mx_mz + \beta z^2 \\
&= (x_1 + \alpha_2z)(x_2 + \alpha_1z) + \dots + (x_{r-1} + \alpha_rz)(x_r + \alpha_{r-1}z) \\
&\quad + z(\alpha_{r+1}x_{r+1} + \dots + \alpha_mx_m) + \underbrace{(\beta - \alpha_1\alpha_2 - \dots - \alpha_{r-1}\alpha_r)}_{\theta} z^2
\end{aligned}$$

If there exists $i > r$ such that $\alpha_i \neq 0$, $R = R + 2$ and $\omega_Q = 2$.

If for all $i > r$, $\alpha_i = 0$ and $\theta = 0$, $R = r$ et $\omega_Q = 2$.

If for all $i > r$, $\alpha_i = 0$ and $\theta \neq 0$, $R = r + 1$ et $\omega_Q = 1$.

Hence $d(q_0, R_q(1, m)) = (q - 1)q^{m-1} + q^{m-\frac{r}{2}-1} - q^{m-\frac{r}{2}}$.

- If r is even and $\omega_{q_0} = 0$, $|q_0 + \alpha_1x_1 + \dots + \alpha_mx_m + \beta| = (q - 1)q^{m-1} - q^{m-\frac{r}{2}-1} - (\omega_Q - 1)q^{m-\frac{r}{2}}$. By a linear transformation, q_0 can be reduced to $x_1x_2 + \dots + x_{r-3}x_{r-2} + ax_{r-1}^2 + bx_r^2 + cx_{r-1}x_r$ with $ax^2 + cx + b$ irreducible.

$$\begin{aligned}
Q &= x_1x_2 + \dots + x_{r-3}x_{r-2} + ax_{r-1}^2 + bx_r^2 + cx_{r-1}x_r + \alpha_1x_1z + \dots + \alpha_mx_mz + \beta z^2 \\
&= (x_1 + \alpha_2z)(x_2 + \alpha_1z) + \dots + (x_{r-3} + \alpha_{r-2}z)(x_{r-2} + \alpha_{r-3}z) + ax_{r-1}^2 \\
&\quad + bx_r^2 + cx_{r-1}x_r + z(\alpha_{r-1}x_{r-1} + \dots + \alpha_mx_m) + \underbrace{(\beta - \alpha_1\alpha_2 - \dots - \alpha_{r-3}\alpha_{r-2})}_{\theta} z^2
\end{aligned}$$

If there exists $i > r$ such that $\alpha_i \neq 0$, $R = r + 2$ and $\omega_Q = 0$.

Assume that for all $i > r$, $\alpha_i = 0$.

First, we study the case where q is odd.

Since $ax^2 + cx + b$ is irreducible, we have $a \neq 0$ and $\Delta = b - \frac{c^2}{4a} \neq 0$.

$$\begin{aligned}
Q &= (x_1 + \alpha_2z)(x_2 + \alpha_1z) + \dots + (x_{r-3} + \alpha_{r-2}z)(x_{r-2} + \alpha_{r-3}z) \\
&\quad + a(x_{r-1} + \frac{c}{2a}x_r + \frac{\alpha_{r-1}}{2a}z)^2 + \Delta x_r^2 + (\alpha_r - \frac{c\alpha_{r-1}}{2a})x_rz + (\theta - \frac{\alpha_{r-1}^2}{4a})z^2 \\
&= (x_1 + \alpha_2z)(x_2 + \alpha_1z) + \dots + (x_{r-3} + \alpha_{r-2}z)(x_{r-2} + \alpha_{r-3}z) \\
&\quad + a(x_{r-1} + \frac{c}{2a}x_r + \frac{\alpha_{r-1}}{2a}z)^2 + \Delta(x_r + \frac{2a\alpha_r - c\alpha_{r-1}}{4a\Delta})^2 \\
&\quad + (\theta - \frac{\alpha_{r-1}^2}{4a} - \frac{(2a\alpha_r - c\alpha_{r-1})^2}{16a^2\Delta})z^2
\end{aligned}$$

If $\theta \neq \frac{\alpha_{r-1}^2}{4a} + \frac{(2a\alpha_r - c\alpha_{r-1})^2}{16a^2\Delta}$, $R = r + 1$ and $\omega_Q = 1$.

If $\theta = \frac{\alpha_{r-1}^2}{4a} + \frac{(2a\alpha_r - c\alpha_{r-1})^2}{16a^2\Delta}$, $R = r$ and $\omega_Q = 0$, since $ax^2 + cx + b$ is irreducible.

Then we study the case where q is even.

Since $ax^2 + cx + b$ is irreducible, $c \neq 0$. So we have

$$Q = (x_1 + \alpha_2 z)(x_2 + \alpha_1 z) + \dots + (x_{r-3} + \alpha_{r-2} z)(x_{r-2} + \alpha_{r-3} z) \\ + c(x_{r-1} + \frac{\alpha_r}{c} z)(x_r + \frac{\alpha_{r-1}}{c} z) + \left(\sqrt{a}x_{r-1} + \sqrt{b}x_r + \sqrt{\theta - \frac{\alpha_{r-1}\alpha_r}{c}}z \right)^2$$

If $c^2\theta \neq a\alpha_r^2 + b\alpha_{r-1}^2 + c\alpha_{r-1}\alpha_r$, $R = r + 1$ and $\omega_Q = 1$.

If $c^2\theta = a\alpha_r^2 + b\alpha_{r-1}^2 + c\alpha_{r-1}\alpha_r$,

$$Q = (x_1 + \alpha_2 z)(x_2 + \alpha_1 z) + \dots + (x_{r-3} + \alpha_{r-2} z)(x_{r-2} + \alpha_{r-3} z) \\ + c(x_{r-1} + \frac{\alpha_r}{c} z)(x_r + \frac{\alpha_{r-1}}{c} z) + \left(\sqrt{a}x_{r-1} + \sqrt{b}x_r + \left(\frac{\sqrt{a}}{c}\alpha_r + \frac{\sqrt{b}}{c}\alpha_{r-1} \right)z \right)^2 \\ = (x_1 + \alpha_2 z)(x_2 + \alpha_1 z) + \dots + (x_{r-3} + \alpha_{r-2} z)(x_{r-2} + \alpha_{r-3} z) \\ + c(x_{r-1} + \frac{\alpha_r}{c} z)(x_r + \frac{\alpha_{r-1}}{c} z) + a(x_{r-1} + \frac{\alpha_r}{c} z)^2 + b(x_r + \frac{\alpha_{r-1}}{c} z)^2$$

so $R = r$ et $\omega_Q = 0$.

Hence $d(q_0, R_q(1, m)) = (q - 1)q^{m-1} - q^{m-\frac{r}{2}-1}$.

5 Bounds of $\rho(1, m)$

We use the general upper bound to find an upper bound to $\rho(1, m)$:

Proposition 12 *For all q , $m \geq 0$, we have*

$$\rho(1, m) \leq (q - 1)q^{m-1} - q^{\frac{m}{2}-1}.$$

Proof : $R_q(1, m)$ is self-complementary, so, by theorem 7, it is enough to show that $R_q(1, m)$ has strength 2.

Let $y = (y_1, \dots, y_m)$ and $z = (z_1, \dots, z_m)$ two different fixed elements of \mathbb{F}_q^m .

Let $f, g \in R_q(1, m)$, we say that f is equivalent to g ($f \sim g$) if and only if $f(y) = g(y)$ and $f(z) = g(z)$.

Let $f(x) = a_1x_1 + \dots + a_mx_m + b$. Let $g = a_1x_1 + \dots + a_mx_m + \beta$ such that $f \sim g$, then

$$\begin{cases} \alpha_1 y_1 + \dots + \alpha_m y_m + \beta = a_1 y_1 + \dots + a_m y_m + b \\ \alpha_1 z_1 + \dots + \alpha_m z_m + \beta = a_1 z_1 + \dots + a_m z_m + b \end{cases} \\ \Leftrightarrow \begin{pmatrix} y_1 & \dots & y_m & 1 \\ z_1 & \dots & z_m & 1 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \\ \beta \end{pmatrix} = \begin{pmatrix} a_1 y_1 + \dots + a_m y_m + b \\ a_1 z_1 + \dots + a_m z_m + b \end{pmatrix}$$

Since $z \neq y$, this system has rank 2, and so there are q^{m-1} solutions.

Furthermore, $\text{Card}(R_q(1, m)) = q^{m+1}$, and $\frac{q^{m+1}}{q^{m-1}} = q^2 = \text{Card}(\mathbb{F}_q^2)$.

Hence $R_q(1, m)$ has strength 2.

□

Proposition 13 *For all q , $m \geq 0$, we have*

$$\rho(1, m) \geq (q - 1)q^{m-1} - q^{\lceil \frac{m}{2} \rceil - 1}.$$

Proof : We have

$$\rho(1, m) \geq \rho_2(1, m),$$

and by theorem 2,

$$\rho_2(1, m) = (q-1)q^{m-1} - q^{\lceil \frac{m}{2} \rceil - 1},$$

which gives the result. □

Remark : $\rho(1, 1) = q - 2$.

Indeed, by proposition 13, $\rho(1, 1) \geq q - 2$. Furthermore, for all $g \in B_1^q$, we consider $f(x) = g(x) - (ax + b)$ with $a = g(1) - g(0)$ and $b = g(0)$; f has at least two roots (0 and 1) so for all $g \in B_1^q$, $d(g, R_q(1, 1)) \leq q - 2$. Hence $\rho(1, 1) \leq q - 2$.

Combining proposition 12 and 13 we get the following :

Corollary 14 *For all q , if m is even, then*

$$\rho(1, m) = (q-1)q^{m-1} - q^{\frac{m}{2}-1}.$$

Proof : For m even, $(q-1)q^{m-1} - q^{\lceil \frac{m}{2} \rceil - 1} = (q-1)q^{m-1} - q^{\frac{m}{2}-1}$. □

Remark : Furthermore, we have shown that $\rho_2(1, m) = (q-1)q^{m-1} - q^{\lceil \frac{m}{2} \rceil - 1}$ and that $\rho_2(1, m)$ is reached for $f(x) = x_1x_2 + \dots + x_{m-3}x_{m-2} + ax_{m-1}^2 + bx_m^2 + cx_{m-1}x_m$ with $ax^2 + cx + b$ irreducible over \mathbb{F}_q . So, since for m even $\rho(1, m) = \rho_2(1, m)$, we get that $\rho(1, m) = d(f, R_q(1, m))$.

6 Calculation of $\rho(1, 3)$ for $q = 3$

From now, we assume that $q = 3$.

Theorem 15 *For $q = 3$, $\rho(1, 3) = 16$.*

Proof : By theorem 3, $15 \leq \rho(1, 3) \leq 16$. Furthermore, if $\rho(1, 3) = 16$, there exists $f \in B_m^q$ such that $d(f, R_3(1, 3)) = 16$ and necessarily, degree of f is greater than 2 since, by theorem 2, $\rho_2(1, 3) = 15$. Using all these restrictions, we use Magma

Algorithm 1

```

K:=GF(3);
P<x,y,z>:=PolynomialRing(K,3);
R1:=[a*x+b*y+c*z+d : a in K, b in K, c in K, d in K];
M:=15;
L:=[0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0];

ad:=function(L); i:=1; r:=true;
while i le #L and r do
if L[i]+1 eq 3 then i:=i+1; L[i-1]:=0;
  else r:=false; L[i]:=L[i]+1; end if; end while;
  return L;
end function;

while M eq 15 and L[23] le 1 do
pol:=L[1]*z^2+L[2]*y*z+L[3]*y^2+L[4]*x*z+L[5]*x*y+L[6]*x^2

```



```

+L[7]*y*z^2+L[8]*y^2*z+L[9]*x*z^2+L[10]*x*y*z+L[11]*x*y^2
+L[12]*x^2*z+L[13]*x^2*y+L[14]*y^2*z^2+L[15]*x*y*z^2
+L[16]*x*y^2*z+L[17]*x^2*z^2+L[18]*x^2*y*z+L[19]*x^2*y^2
+L[20]*x*y^2*z^2+L[21]*x^2*y*z^2+L[22]*x^2*y^2*z
+L[23]*x^2*y^2*z^2;
k:=1; m:=16;
while k le #R1 and m eq 16 do
if Evaluate(R1[k],<0,0,0>) ne 0 then r:=1; else; r:=0; end if;
p:=<1,0,0>;
while r lt 16 and p ne <0,0,0> do
if Evaluate(pol+R1[k],p) ne 0 then r:=r+1; p:=ad(p);
else p:=ad(p); end if; end while;
if r lt m then m:=r; end if;
k:=k+1; end while;
if m gt M then M:=m; else L:=ad(L); end if; end while;

print(M);
print(L);

```

We get that $d(y^2 + xy + y^2z + xyz + y^2z^2 + x^2z^2, R_3(1, 3)) = 16$.

□

Proposition 16 *There is no $f \in R_3(6, 4) \setminus R_3(4, 3)$ such that $d(f, R_3(1, 3)) = 16$.*

Lemma 17 *For $q \geq 3$, if $f \in R_q(m(q-1), m) \setminus R_q(m(q-1)-1, m)$ then there exists $\sigma \in \text{GA}_m(\mathbb{F}_q)$, $a \in \mathbb{F}_q^*$ and $r \in R_q(m(q-1)-2, m)$ such that*

$$\sigma.f = a \prod_{i=1}^m x_i^{q-1} + r$$

Proof : We write f as

$$f = a \prod_{i=1}^m x_i^{q-1} + \sum_{i=1}^m a_i \prod_{k \neq i} x_k^{q-1} x_i^{q-2} + s$$

where $a, a_i \in \mathbb{F}_q$, $a \neq 0$ and $s \in R_q(m(q-1)-2, m)$.

Let $\omega \in \mathbb{F}_q^m$ then

$$\begin{aligned}
1_\omega &= \prod_{i=1}^m (1 - (x_i - \omega_i)^{q-1}) \\
&= \prod_{i=1}^m \left(1 - \sum_{k=1}^{q-1} \binom{q-1}{k} x_i^k (-\omega_i)^{q-1-k} \right) \\
&= (-1)^m \prod_{i=1}^m x_i^{q-1} + (-1)^m \sum_{i=1}^m \omega_i \prod_{k \neq i} x_k^{q-1} x_i^{q-2} + t, \quad t \in R_q(m(q-1)-2, m).
\end{aligned}$$

Hence

$$f = (-1)^m a 1_{(a^{-1}a_i)} + r', \quad r' \in R_q(m(q-1)-2, m).$$

Let $\sigma \in \text{GA}_m(\mathbb{F}_q)$,

$$\sigma.f = (-1)^m a 1_{\sigma^{-1}(a^{-1}a_i)} + \sigma.r', \quad r' \in R_q(m(q-1)-2, m).$$

We choose σ such that $\sigma^{-1}(a^{-1}a_i) = 0$.

$$1_0 = \prod_{i=1}^m (1 - x_i^{q-1}) = (-1)^m \prod_{i=1}^m x_i^{q-1} + u,$$

$$u \in R_q((m-1)(q-1), m) \subset R_q(m(q-1)-2, m) \quad \text{since } q \geq 3$$

Finally, since $\text{Aut}(R_q(m(q-1)-2, m)) = \text{GA}_m(\mathbb{F}_q)$, we get

$$\sigma.f = a \prod_{i=1}^m x_i^{q-1} + r, \quad r \in R_q(m(q-1)-2, m).$$

□

Lemma 18 *If $f \in R_q(m(q-1)-1, m) \setminus R_q(m(q-1)-2, m)$ then there exists $\sigma \in \text{GL}_m(\mathbb{F}_q)$ and $r \in R_q(m(q-1)-2, m)$ such that*

$$\sigma.f = \prod_{i=1}^{m-1} x_i^{q-1} x_m^{q-2} + r$$

Proof : We write $f = \sum_{i=1}^m \alpha_i \prod_{k \neq i} x_k^{q-1} x_i^{q-2} + t$, $t \in R_q(m(q-1)-2, m)$.

Let $b \in \mathbb{F}_q^m$,

$$\begin{aligned} 1_0 - 1_b &= \prod_{i=1}^m (1 - x_i^{q-1}) - \prod_{i=1}^m (1 - (x_i - b_i)^{q-1}) \\ &= \prod_{i=1}^m (1 - x_i^{q-1}) - \prod_{i=1}^m \left(1 - \sum_{k=1}^{q-1} \binom{q-1}{k} x_i^k (-b_i)^{q-1-k}\right) \\ &= (-1)^{m+1} \sum_{i=1}^m b_i \prod_{k \neq i} x_k^{q-1} x_i^{q-2} + s, \quad s \in R_q(m(q-1)-2, m). \end{aligned}$$

D'où $f = 1_0 - 1_{((-1)^{m+1}\alpha_i)} + r'$, $r' \in R_q(m(q-1)-2, m)$.

Let $\sigma \in \text{GL}_m(\mathbb{F}_q)$ then

$$\sigma.f = 1_{\sigma^{-1}(0)} - 1_{\sigma^{-1}((-1)^{m+1}\alpha_i)} + \sigma.r' = 1_0 - 1_{\sigma^{-1}((-1)^{m+1}\alpha_i)} + \sigma.r'$$

Since $f \in R_q(m(q-1)-1, m) \setminus R_q(m(q-1)-2, m)$, $((-1)^{m+1}\alpha_i) \neq 0$. So there exists $\sigma \in \text{GL}_m(\mathbb{F}_q)$ such that

$$\sigma^{-1}((-1)^{m+1}\alpha_i) = \begin{pmatrix} (-1)^{m+1} \\ 0 \\ \vdots \\ 0 \end{pmatrix} = c$$

and

$$\sigma.f = 1_0 - 1_c + \sigma.r' = \prod_{i=1}^{m-1} x_i^{q-1} x_m^{q-1} + r$$

with $r \in R_q(m(q-1)-2, m)$ since $\text{Aut}(R_q(m(q-1)-2, m)) = \text{GA}_m(\mathbb{F}_q)$.

□

Proof of proposition : By lemma 17 and 18, the following algorithms on Magma give the result.

Algorithm 2 (degré 6)

```

K:=GF(3);
P<x,y,z>:=PolynomialRing(K,3);
R1:=[a*x+b*y+c*z+d : a in K, b in K, c in K, d in K];

ad:=function(L); i:=1; r:=true;
while i le #L and r do
  if L[i]+1 eq 3 then i:=i+1; L[i-1]:=0;
  else r:=false; L[i]:=L[i]+1; end if; end while;
return L;
end function;

L:=[1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0];
while L ne [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0] do
pol:=L[1]*z^2+L[2]*y*z+L[3]*y^2+L[4]*x*z+L[5]*x*y+L[6]*x^2
+L[7]*y*z^2+L[8]*y^2*z+L[9]*x*z^2+L[10]*x*y*z+L[11]*x*y^2
+L[12]*x^2*z+L[13]*x^2*y+L[14]*y^2*z^2+L[15]*x*y*z^2
+L[16]*x*y^2*z+L[17]*x^2*z^2+L[18]*x^2*y*z
+L[19]*x^2*y^2+x^2*y^2*z^2;
k:=1; m:=16;
while k le #R1 and m eq 16 do
if Evaluate(R1[k],<0,0,0>) ne 0 then r:=1; else; r:=0; end if;
p:=<1,0,0>;
while r lt 16 and p ne <0,0,0> do
  if Evaluate(pol+R1[k],p) ne 0 then r:=r+1; p:=ad(p);
  else p:=ad(p); end if; end while;
if r lt m then m:=r; end if;
k:=k+1; end while;
if m gt 15 then print(pol); L:=ad(L); else L:=ad(L); end if; end while;

```

```

K:=GF(3);
P<x,y,z>:=PolynomialRing(K,3);
R1:=[a*x+b*y+c*z+d : a in K, b in K, c in K, d in K];

ad:=function(L); i:=1; r:=true;
while i le #L and r do
  if L[i]+1 eq 3 then i:=i+1; L[i-1]:=0;
    else r:=false; L[i]:=L[i]+1; end if; end while;
  return L;
end function;

L:=[1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0];
while L ne [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0] do
pol:=L[1]*z^2+L[2]*y*z+L[3]*y^2+L[4]*x*z+L[5]*x*y+L[6]*x^2
      +L[7]*y*z^2+L[8]*y^2*z+L[9]*x*z^2+L[10]*x*y*z+L[11]*x*y^2
      +L[12]*x^2*z+L[13]*x^2*y+L[14]*y^2*z^2+L[15]*x*y*z^2
      +L[16]*x*y^2*z+L[17]*x^2*z^2+L[18]*x^2*y*z+L[19]*x^2*y^2+x^2*y^2*z;
k:=1; m:=16;
while k le #R1 and m eq 16 do
if Evaluate(R1[k],<0,0,0>) ne 0 then r:=1; else; r:=0; end if;
p:=<1,0,0>;
while r lt 16 and p ne <0,0,0> do
  if Evaluate(pol+R1[k],p) ne 0 then r:=r+1; p:=ad(p);
    else p:=ad(p); end if; end while;
if r lt m then m:=r; end if;
k:=k+1; end while;
if m gt 15 then print(pol); L:=ad(L); else L:=ad(L); end if; end while;

```

☐

Proposition 19 *All f in $R_3(4, 3)$ such that $d(f, R_3(1, 3)) = 16$ are equivalent under the action of $\text{GA}_3(\mathbb{F}_3)$ and $R_3(1, 3)$ to*

7 Improvement of the lower bound of $\rho(1, m)$ for $q = 3$

Lemma 20 *For all q , for all m ,*

Proof : Let $f \in R_q(1, m+2)$. We can write $f(x_1, \dots, x_{m+2}) = g(x_1, \dots, x_m) + \alpha x_{m+1} + \beta x_{m+2}$, where $g \in R_q(1, m)$ and $\alpha, \beta \in \mathbb{F}_q$.

$$R_q(1, m+2) = \{M(c, \alpha, \beta), c \in R_q(1, m), \alpha \in \mathbb{F}_q, \beta \in \mathbb{F}_q\}$$

where $M(c, \alpha, \beta) = (c, \bar{c}^{\alpha\omega_1}, \dots, \bar{c}^{\alpha\omega_{q-1}}, \bar{c}^{\beta\omega_1}, \bar{c}^{\alpha\omega_1+\beta\omega_1}, \dots, \bar{c}^{\beta\omega_1+\alpha\omega_{q-1}}, \dots, \bar{c}^{\alpha\omega_{q-1}+\beta\omega_{q-1}})$

If v_0 is such that $d(v_0, R_q(1, m)) = \rho(1, m)$, then for all $c \in R_q(1, m)$, $|v_0 + c| \geq \rho(1, m)$.

Let $u = (\bar{v}_0^{\omega_0\omega_0}, \dots, \bar{v}_0^{\omega_0\omega_{q-1}}, \bar{v}_0^{\omega_1\omega_0}, \dots, \bar{v}_0^{\omega_1\omega_{q-1}}, \dots, \bar{v}_0^{\omega_{q-1}\omega_{q-1}}) \in B_{m+2}^q$.

If $\alpha, \beta \in \mathbb{F}_q$ and $c \in R_q(1, m)$, then

$$\begin{aligned} |u + M(c, \alpha, \beta)| &= \sum_{i=0}^{q-1} \sum_{j=0}^{q-1} |\bar{v}_0^{\omega_i\omega_j} + \bar{c}^{\alpha\omega_i+\beta\omega_j}| \\ &= \sum_{i=0}^{q-1} \sum_{j=0}^{q-1} |\bar{v}_0^{(\beta+\omega_i)\omega_j} + \bar{c}^{\alpha\omega_i}| \\ &= q|\bar{c}^{\alpha(-\beta)} + v_0| + \sum_{\omega_i \neq -\beta} \sum_{j=0}^{q-1} |\bar{v}_0^{(\beta+\omega_i)\omega_j} + \bar{c}^{\alpha\omega_i}| \\ &\geq q\rho(1, m) + (q-1)^2 q^m \end{aligned}$$

which gives the result. □

Theorem 21 For $q = 3$ and m an odd integer,

$$\rho(1, m) \geq (q-1)q^{m-1} - \frac{2}{3}q^{\lceil \frac{m}{2} \rceil - 1}$$

Proof : We write $m = 2k + 1$. We prove by induction on u that for $u \leq k$,

$$\rho(1, m) \geq (q-1)(q^{m-1} - q^{m-1-u}) + q^u \rho(1, m-2u).$$

This is true for $u = 0$ and $u = 1$ (lemma 20). Assume that it is true for some $u < k$. Then

$$\begin{aligned} \rho(1, m) &\geq (q-1)(q^{m-1} - q^{m-1-u}) + q^u \rho(1, m-2u) \\ &\geq (q-1)(q^{m-1} - q^{m-1-u}) + q^u ((q-1)^2 q^{m-2u-2} + q\rho(1, m-2u-2)) \\ &\quad \text{(by lemma 20)} \\ &\geq (q-1)q^{m-1} - (q-1)(q - (q-1))q^{m-u-2} + q^{u+1}\rho(1, m-2(u+1)) \\ &\geq (q-1)(q^{m-1} - q^{m-(u+1)-1}) + q^{u+1}\rho(1, m-2(u+1)) \end{aligned}$$

Hence, for $q = 3$ and $u = k-1$, we get :

$$\begin{aligned} \rho(1, m) &\geq (q-1)(q^{m-1} - q^{k+1}) + q^{k-1}\rho(1, 3) \\ &\geq (q-1)q^{m-1} - 2q^{k-1} = (q-1)q^{m-1} - \frac{2}{3}q^{\lceil \frac{m}{2} \rceil - 1} \end{aligned}$$

□

Corollary 22 For $q = 3$, $\rho(1, 5) = 156$

Proof : By theorem 21, $\rho(1, 5) \geq 2 \cdot 3^4 - \frac{2}{3} \cdot 9 = 156$. and by proposition 12, $\rho(1, 5) \leq [2 \cdot 3^4 - 3\sqrt{3}] = 156$. □

References

- [1] E. Berlekamp, L.R. Welch, *Weight distribution of the cosets of the $(32,6)$ Reed-Muller code*, IEEE Transactions on Information Theory, IT-18, n°1 (1972), 203-207.
- [2] L.E. Dickson, *Linear groups*, Dover Publication (1958).
- [3] J. Dieudonné, *La géométrie des groupes classiques*, Springer (1963).
- [4] T. Helleseth, T. Kløve, J. Mykkeltveit, *On the covering radius of binary codes*, IEEE Transactions on Information Theory, IT-24, n°5 (1978), 627-628.
- [5] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford Mathematics Monographs (1998), 117-125.
- [6] X. Hou, *Covering radius of the Reed-Muller code $R(1,7)$ - a simpler proof*, Journal of combinatorial theory, series A 74 (1996), 337-341.
- [7] X. Hou, *Further results on the covering radii of the Reed-Muller codes*, Designs, Codes and cryptography 3 (1993), 167-177.
- [8] W.C. Huffman, V. Pless, *Handbook of coding theory*, vol 2, chapter 16, Elsevier (1998).
- [9] P. Langevin, *On the orphans and covering radius of the Reed-Muller codes*, Lecture Notes in Computer Sciences, vol. 539, Springer (1991), 234-240.